

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF MICHIGAN  
SOUTHERN DIVISION

United States of America,

Civil Case No. 24-cv-12313

Plaintiff,

Honorable

vs.

Magistrate Judge

Cryptocurrency funds from OKX Account  
Identification: UUID: 162225466726559744  
with the affiliated deposit address,  
0x2729a03f2374c48f9f51eed65c3bd1f5cda106e1

Defendant *in Rem*.

---

**Complaint for Forfeiture**

---

Plaintiff, United States of America, by and through its undersigned attorneys, states the following in support of this Complaint for Forfeiture:

**Jurisdiction and Venue**

1. This is an *in rem* civil forfeiture action pursuant to 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C), resulting from violations of 18 U.S.C. § 1343 and 18 U.S.C. § 1956, 1957.

2. This Court has original jurisdiction over this proceeding pursuant to 28 U.S.C. § 1345 because this action is being commenced by the United States of America as plaintiff.

3. This Court has jurisdiction over this forfeiture action under 28 U.S.C. § 1355(b)(1)(A) because acts giving rise to the forfeiture occurred in the Eastern District of Michigan.

4. Venue is proper before this Court under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the government's claims occurred in the Eastern District of Michigan.

5. Venue is also proper before this Court under 28 U.S.C. § 1395 because the action accrued in the Eastern District of Michigan.

**Defendant *in rem***

6. The defendant *in rem* consists of cryptocurrency funds from OKX Account Identification: UUID: 162225466726559744 with the affiliated deposit address, 0x2729a03f2374c48f9f51eed65c3bd1f5cda106e1 (“Defendant Cryptocurrency”).

7. The Defendant Cryptocurrency was seized as proceeds of wire fraud and/or money laundering pursuant to a seizure warrant executed by the United States Secret Service (“USSS”).

**Underlying Criminal Statutes**

8. 18 U.S.C. § 1343 (“Wire Fraud”) prohibits anyone from devising or intending to devise any scheme or artifice to defraud, or to obtain money or property by means of false or fraudulent pretenses, representations, or promises, to

transmit or cause to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice.

9. 18 U.S.C. § 1956(a)(1)(B)(i) makes it a federal offense for anyone, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, to conduct or attempt to conduct such a financial transaction which, in fact, involves the proceeds of specified unlawful activity, knowing that the transaction is designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds.

10. 18 U.S.C. § 1957 makes it unlawful for any person to knowingly engage or attempt to engage in a monetary transaction in criminally derived property of a value greater than \$10,000 if the property is, in fact, derived from specified unlawful activity.

### **Statutory Basis for Civil Forfeiture**

11. 18 U.S.C. § 981(a)(1)(A) provides for civil forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956, 1957, or 1960, or any property traceable to such property.

12. 18 U.S.C. § 981(a)(1)(C) provides for civil forfeiture of any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of a specified unlawful activity, which includes violations of 18 U.S.C.

§ 1343 (Wire Fraud), 18 U.S.C. § 1956 (Money Laundering), and 18 U.S.C. § 1957 (Spending).

**Factual Basis in Support of Forfeiture**

13. The Defendant Cryptocurrency is forfeitable to the United States as property that constitutes or is derived from the proceeds of wire fraud in violation of 18 U.S.C. § 1343 and as property involved in money laundering. The facts supporting this evidentiary determination include, but are not limited to, the following:

a. On or about March 13, 2023, an individual (“victim”) contacted the United States Secret Service (“USSS”) through its public facing webpage and reported being the victim of an online Pig Butchering scam and lost just under \$320,000.00. A review of the victim’s bank transactions revealed the actual amount to be \$311,300.00.

b. The victim, a resident of Troy, Michigan advised USSS that toward the end of October 2022 he started a conversation with an individual from a hiking group on Facebook named “An Na Lise.” The victim stated the conversations were initially about hiking and eventually led to discussions about investing and investing in crypto mining.

c. Open-source research revealed that this “An Na Lise,” who was in contact with the victim on Facebook has changed their Facebook profile

picture and name to “Kimberly Maisie.” The profile photo for “Kimberly Maisie” changed to different women over the course of a few weeks.

d. On or about December 14, 2022, the victim wired \$8,100.00 to Metropolitan Commercial Bank (“MCB”) to be deposited into a Crypto.com account. The victim purchased USDT and had it transferred to dbex-coin.net, which victim believed was a legitimate cryptocurrency trading platform. All of this was done with step-by-step instruction from “An Na Lise.”

e. After seeing purported quick growth on dbex-coin.net, victim withdrew \$204,500 from an IRA to invest in a longer-term mining pool. Victim was persuaded several times to send more money. For example, on or about January 11, 2023, victim sent another \$48,500 for a twelve-day investment.

f. Investigation revealed that victim sent five (5) transactions from the victim’s Bank of America Account into a Crypto.com Account ending in 6407 (Crypto 6407). See chart below.

<u>Date</u> <u>Received</u>	<u>Amonnt</u>	<u>Beneficiary</u>	<u>Notes</u>
12/14/22	8,100.00	MCB FORIS / Crypto.com	BOA wire on 12/02/22
12/22/22	27,000.00	MCB FORIS / Crypto.com	BOA wire on 12/22/22
12/27/22	177,500.00	MCB FORIS / Crypto.com	BOA wire 12/24/22
1/11/23	48,500.00	MCB FORIS / Crypto.com	BOA wire on 01/11/23
1/25/23	50,200.00	MCB FORIS / Crypto.com	BOA wire on 01/25/23
<b>Total</b>	311,300.00	Sent from BOA to FORIS	

g. The victim transferred a total of \$311,300.00 to Crypto 6407. Account records show that after receiving the funds into Crypto 6407, the funds were swapped from US dollars to USDC, which is a type of cryptocurrency referred to as a stablecoin with a 1:1 value ratio with the US dollar.

h. A review of records obtained from MCB FORIS/Crypto.com reveals that once the funds were swapped to USDC, they were sent in five (5) separate transactions to other cryptocurrency addresses that were not in the name of, or under the control, of the victim.

i. On or about January 25, 2023, the victim submitted a withdrawal request for \$230,000.00 but was told that based on the “profit” earned on the “investment,” the victim would have to pay an additional \$86,000.00 in taxes to complete the withdrawal. The victim was also told that if they sent

\$100,000.00, the victim would never have to pay any short-term capital gain or any penalties for as long as the victim had an account.

j. Victim did not have funds to pay the “tax” to complete the withdrawal. “An Na Lise” suggested that victim go to Best Egg or Lending Tree to secure the funds. Instead, the victim borrowed \$50,000 from victim’s 94 year old mother and whomever else would lend him the funds. At this point, victim’s daughter informed victim that he had likely been defrauded.

k. The victim pleaded with the person he had been in contact with at dbex and “An Na Lise,” to return any portion of the funds but was ultimately blocked from accessing the dbex-coin.net account.

l. A Detroit USSS Investigative Analyst (IA), who has received specialized training conducting cryptocurrency investigations which require analysis of cryptocurrency transactions on the blockchain, was able to trace some of the victim’s original funds through a complicated series of cryptocurrency transactions to a series of unknown addresses.

m. A review of records by USSS, in addition to the Cryptocurrency tracing conducted, showed the following transactions: \$48,500.00 US dollars was sent from the BOA account to Crypto 6407 on January 11, 2023. \$48,500.00 US dollars were then exchanged for 48,490 USDC (fee included) and sent to USDC address

0xAaD4D89CBa71dF0d0DBc3E99AD5cCa169F86B678 (USDC/T 0xAa) on January 12, 2023.

n. Blockchain analysis conducted on USDC/T 0xAa shows that on January 12, 2023, a cryptocurrency “swap” took place in a transaction that swapped USDC for USDT. USDC/T 0xAa sent 48,490 USDC to address 0x4a14347083b80e5216ca31350a2d21702ac3650d (USDC/T 0x4a). To complete the “swap,” USDC/T 0x4a sent the 48,490 USDC to swap address 0xbebc44782c7db0a1a60cb6fe97d0b483032ff1c7 (SWAP 0xbe). SWAP 0xbe completed the “swap” and sent 48,481.827518 USDT back to USDC/T 0x4a. USDC/T 0x4a then sent 48,462.434786 USDT to the initial address, USDC/T 0xAa.

o. “Swaps” of cryptocurrency are methods for actors to promote obfuscation on the blockchain and strengthen money laundering tactics to avoid law enforcement intervention. Wallets that engage in these “swaps” are known to have relationships with “imtoken” and “Tokenlon.” These are known Asia based service that charge for controllers to token swap their coins. Imtoken and Tokelon are known to be run and utilized by several illicit actors to promote money laundering because the service is a de-fi or light service that does not require any identification documents and is in countries that are free from the reach of most Financial Action Task Force



countries. The services also operate with a light feature that allows the user to hold the private keys which prevents law enforcement from having the ability to freeze or seize accounts.

p. On January 12, 2023, after confirming the deposit of 48,462.434786 USDT into USDC/T 0xAa through blockchain analysis, USDC/T 0xAa sent 3,000 USDT to an unknown address. A few minutes later 46,471.688758 USDT was sent from USDC/T 0xAa to unknown address 0xee0ab49DCfCcDF000E810794a410040c3B7f7365 (USDT 0xee).

q. On January 12, 2023, blockchain analysis confirmed USDT 0xee received 46,471.688758 USDT in which the next withdrawal from USDT 0xee was 77,470 USDT into address 0x1e13Dd13287DC0659820D45Ce399F460EeC7D6A3 (USDT 0x1e).

r. On January 16, 2023, USDT 0x1e receives the 77,470 USDT and on the same day sends 93,800 USDT to address 0xcFBf16eac93650F167658F548ceb4A697187cDA5 (USDT 0xcF). It should be noted that the address USDT 0x1e receives deposits in 4 other transactions directly tied to funds sent by the victim. \$92,307 USDT was sent from 0xcF to 0x6416F85a6328D319eA6caE7f652Deaa036d47a45 (USDT 0x64).

s. From January 16, 2023, to February 17, 2023, additional transactions took place, including the following:

- On January 16, 2023: USDT 0x64 sent 92,300 USDT to 0x29014ee2dB21953CF7F5Bd1a3291498534748F87 (USDT 0x29).
- On January 18, 2023: USDT 0x29 sent 31,519 USDT to 0xF5cCEe4C6f16DbCC15d5CAC940305862bC98f2e (USDT 0xF).
- On February 17, 2023: Withdrawals of 10 USDT and 199,990 USDT were sent from USDT 0xF to OKX address 0x2729a03F2374c48f9f51eeD65c3Bd1f5Cda106E1 (OKX 0x27).

t. OKX 0x27 is associated with user UUID 162225466726559744 and ID Number 342222199008071680.

u. OKX is a full-service cryptocurrency exchanger and offers service to account holders that involve facilitating the purchase, sale and transfer of a variety of digital currencies.

v. OKX 0x27 was created on March 28, 2021. Based on account records, between March 2021 and April 2023, OKX 0x27 received approximately \$4.6 million in USDT. During the same time frame, approximately \$4.3 million USDT was withdrawn from the wallet.

w. The unknown wallet controller of OKX 0x27 utilized private addresses for the token movements which is indicative of money laundering tactics that are used to conceal and disguise the original source of the funds. Private wallets are non-custodial wallets, meaning the owner, as opposed to

the host, controls the private keys and therefore all associated funding without oversight or financial regulation. Private non-custodial wallets can be held in numerous forms such as, wallet applications on computers and cell phones, cold storage devices not connected to the internet and paper wallets.

x. As described above, funds originally deposited by the victim were moved through various cryptocurrency wallets. Conducting numerous transactions within a short period of time and using cryptocurrency swaps are methods to conceal or disguise the source of the funds. The number of hops described in the preceding paragraphs are a strong indication that the victim's funds were moved in a manner intended to conceal or disguise their nature, location, source, ownership, or control.

y. Research was conducted through the Internet Crime Complaint Center (IC3), which is a division of the Federal Bureau of Investigation that gives victims a convenient and easy way to report/alert authorities of criminal or civil violations on the internet. Research in IC3 shows that there are numerous reports of a Pig Butchering scheme which utilized the trading platform "dbex-coin.net." There are approximately 45 IC3 reports in which individuals identified sending funds to unknown wallet addresses related to cryptocurrency investments. In every instance, the individuals reported

being a victim of the “dbex” fraud scheme. Many of these reports indicate they were also defrauded by the same website, dbex-coin.net.

z. Research was also performed through the Consumer Sentinel Network, which is a database comprised of consumer complaints. Consumer Sentinel Network recorded a total of 9 complaints, dating from 10/31/2022 - 03/01/2023, related to the Pig Butchering scheme associated with “dbex-coin.net” with a total victim loss of \$1,397,621. In total, there are approximately 27 victim complaints regarding the “dbex” scheme with \$3,322,702 in losses from 07/01/2022 - 03/24/2023.

aa. On April 21, 2023, a warrant was issued by a federal magistrate judge in the Eastern District of Michigan to seize Defendant Cryptocurrency and executed by USSS.

### **Claim**

14. Plaintiff re-alleges and incorporates by reference each and every allegation contained in paragraphs one through 13 above, including all their subparts.

15. Based upon the facts outlined above and the applicable law, the Defendant Cryptocurrency is forfeitable to the United States under 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C), as proceeds of wire fraud and as property involved in money laundering.

**Conclusion and Relief**

Plaintiff respectfully requests that a warrant for arrest of the defendant *in rem* be issued; that due notice be given to all interested parties to appear and show cause why the forfeiture should not be decreed; that judgment be entered declaring that the defendant *in rem* be condemned and forfeited to the United States of America for disposition according to law; and that the United States be granted such other relief as this Court may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

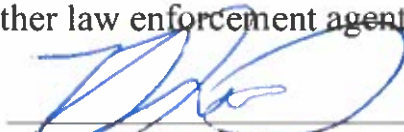
DAWN N. ISON  
United States Attorney

S/Adriana Dydell  
Adriana Dydell (CA 239516)  
Assistant U.S. Attorney  
211 W. Fort Street, Ste. 2001  
Detroit, Michigan 48226  
(313) 226-9125  
Adriana.Dydell@usdoj.gov

Dated: September 5, 2024

**VERIFICATION**

I, Timitre Kyriakides, am a Special Agent with the United States Secret Service. I have read the foregoing Complaint for Forfeiture and assert under penalty of perjury that the facts contained therein are true to the best of my knowledge and belief, based upon knowledge possessed by me and/or on information that I received from other law enforcement agents and/or officers.



---

Timitre Kyriakides, Special Agent  
United States Secret Service

Dated: August 6, 2024